Fortinet NSE 4 - FortiOS 7.0

1. Which two statements about FortiGate FSSO agentless polling mode are true? (Choose two.)

- [ ] A. FortiGate uses the AD server as the collector agent.
- [ ] B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- [ ] C. FortiGate does not support workstation check.
- [ ] D. FortiGate directs the collector agent to use a remote LDAP server.

Answer(s): B D

---

2. FortiGuard categories can be overridden and defined in different categories. To create a web rating override for example.com home page, the override must be configured using a specific syntax.
Which two syntaxes are correct to configure web rating override for the home page? (Choose two.)

- [ ] A. www.exaple.com
- [ ] B. www.example.com/index.html
- [ ] C. example.com
- [ ] D. www.example.com:443

Answer(s): A C

---

3. Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).
Exhibit A.

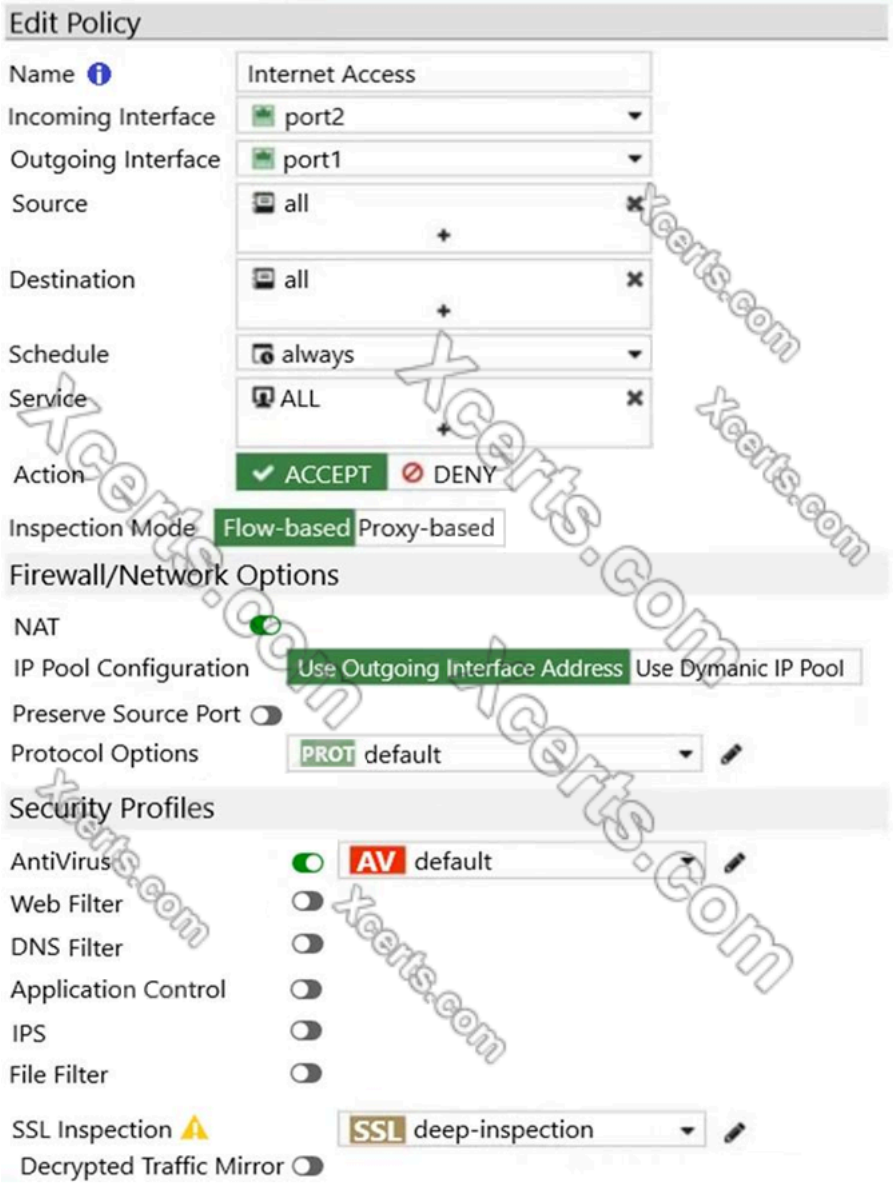

Edit Policy
Name
Internet Access
Incoming Interface
port2
Outgoing Interface
port1
Source
all
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall/Network Options
NAT
IP Pool Configuration
Use Outgoing Interface Address
Use Dymanic IP Pool
Preserve Source Port
Protocol Options
PROT
default
Security Profiles
AntiVirus
AV
default
Web Filter
DNS Filter
Application Control
IPS
File Filter
SSL Inspection
SSL
deep-inspection
Decrypted Traffic Mirror

Exhibit B.

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

A. The flow-based Inspection is used, which resets the last packet to the user.

B. The volume of traffic being inspected is too high for this model of FortiGate.

C. The firewall policy performs the full content inspection on the file.

D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

Answer(s): A

---

4. Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

- [ ] A. FortiSandbox
- [ ] B. FortiCloud
- [ ] C. FortiSIEM
- [ ] D. FortiCache
- [ ] E. FortiAnalyzer

Answer(s): B C E

---

5. Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

A. NetAPI polling can increase bandwidth usage in large networks.

B. The NetSessionEnum function is used to track user logouts.

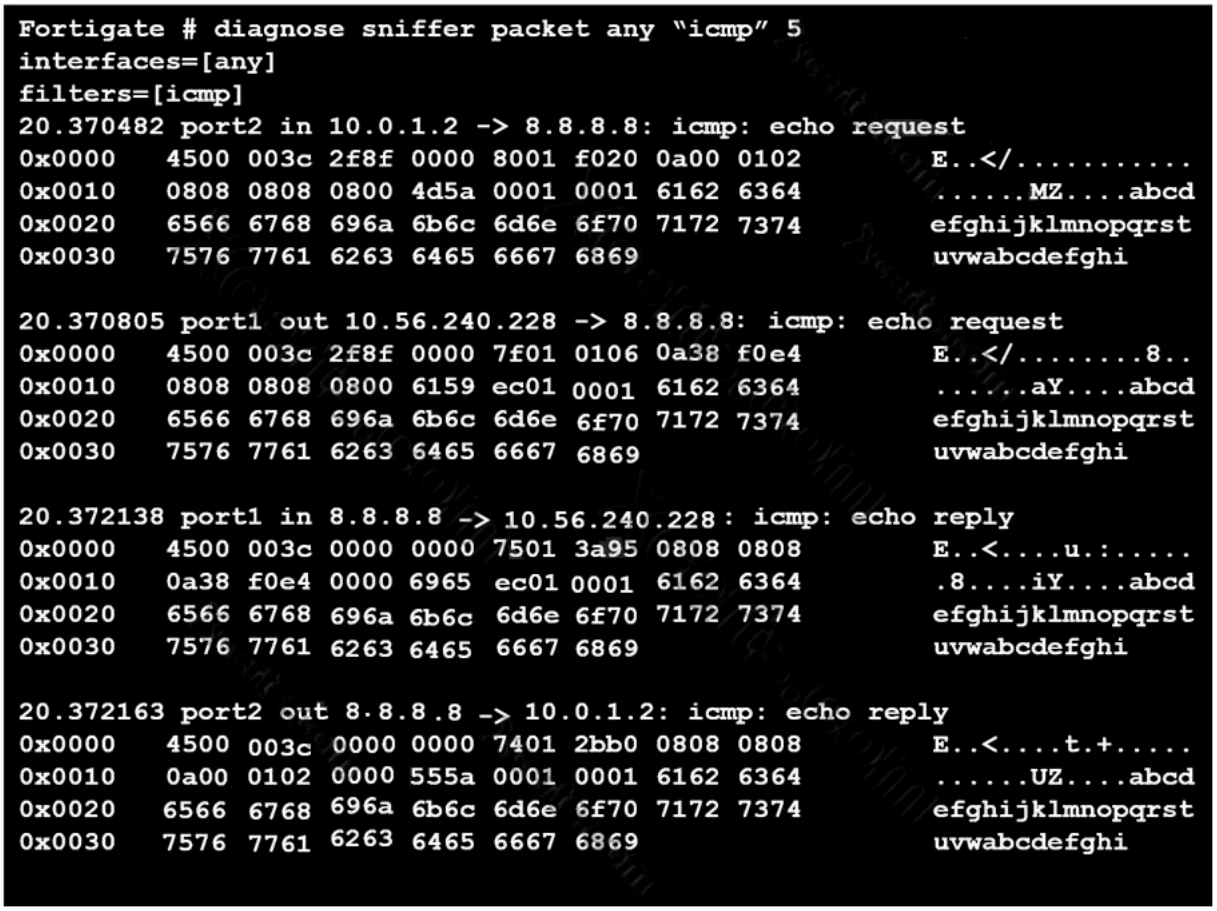
C. The collector agent must search security event logs.

D. The collector agent uses a Windows API to query DCs for user logins.

Answer(s): B

---

6. Refer to the exhibit.



```
Fortigate # diagnose sniffer packet any "icmp" 5
interfaces=[any]
filters=[icmp]
20.370482 port2 in 10.0.1.2 -> 8.8.8.8: icmp: echo request
0x0000   4500 003c 2f8f 0000 8001 f020 0a00 0102        E..</.....
0x0010   0808 0808 0800 4d5a 0001 0001 6162 6364        ......MZ....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.370805 port1 out 10.56.240.228 -> 8.8.8.8: icmp: echo request
0x0000   4500 003c 2f8f 0000 7f01 0106 0a38 f0e4        E..</........8..
0x0010   0808 0808 0800 6159 ec01 0001 6162 6364        ......aY....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.372138 port1 in 8.8.8.8 -> 10.56.240.228: icmp: echo reply
0x0000   4500 003c 0000 0000 7501 3a95 0808 0808        E..<....u.:.....
0x0010   0a38 f0e4 0000 6965 ec01 0001 6162 6364        .8....iY....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.372163 port2 out 8.8.8.8 -> 10.0.1.2: icmp: echo reply
0x0000   4500 003c 0000 0000 7401 2bb0 0808 0808        E..<....t.+.....
0x0010   0a00 0102 0000 555a 0001 0001 6162 6364        ......UZ....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi
```

An administrator is running a sniffer command as shown in the exhibit.
Which three pieces of information are included in the sniffer output? (Choose three.)

- [ ] A. Interface name
- [ ] B. IP header
- [ ] C. Application header
- [ ] D. Packet payload
- [ ] E. Ethernet header

Answer(s): A B D

---

7. Refer to the exhibits.
Exhibit A.

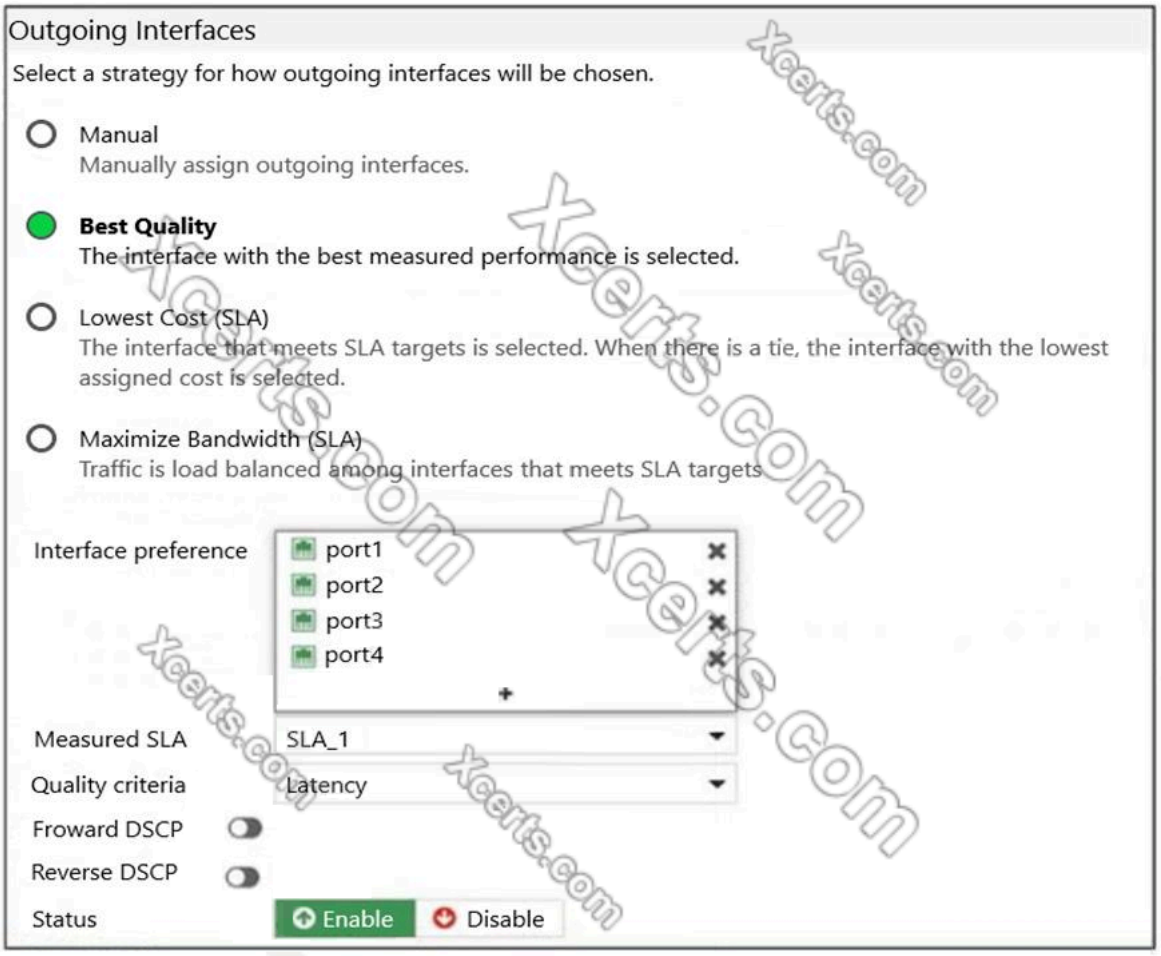


Exhibit B.

```
NGFW-1 # diagnose sys sdwan health-check
Health Check(SLA-1):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2
Seq(2 port2): state(alive), packet-loss(0.000%) latency(54.349), jitter(4
Seq(3 port3): state(alive), packet-loss(0.100%) latency(32.683), jitter(5
Seq(4 port4): state(alive), packet-loss(2.010%) latency(48.881), jitter(4
```

The exhibit contains the configuration for an SD-WAN Performance SLA, as well as the output of diagnose sys virtual-wan-link health-check.
Which interface will be selected as an outgoing interface?

A. port2

B. port3

C. port4

D. port1

Answer(s): D

---

8. An administrator does not want to report the logon events of service accounts to FortiGate.
What setting on the collector agent is required to achieve this?

A. Add user accounts to the Ignore User List.

B. Add the support of NTLM authentication.

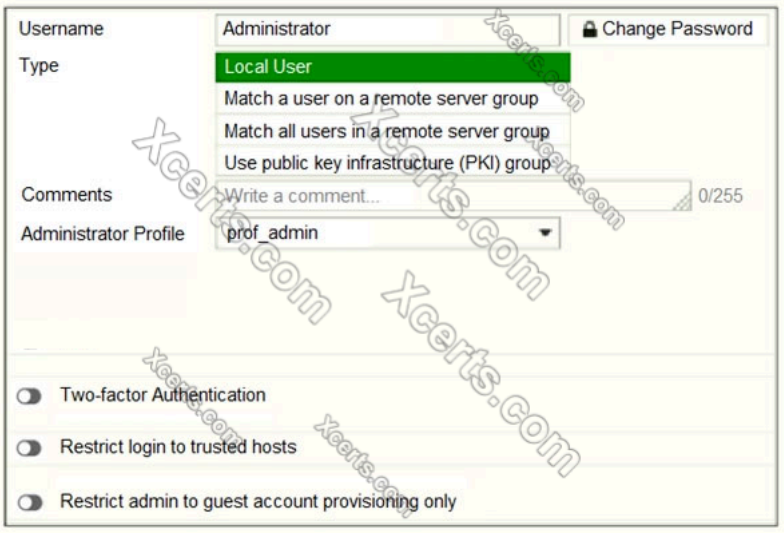
C. Add user accounts to the FortiGate group filter.

D. Add user accounts to Active Directory (AD).

Answer(s): A

---

9. Refer to the exhibit.



The global settings on a FortiGate device must be changed to align with company security policies.
What does the Administrator account need to access the FortiGate global settings?

A. Enable two-factor authentication

B. Change Administrator profile

C. Change password

D. Enable restrict access to trusted hosts.

Answer(s): B

---

10. Which two statements are true about the Security Fabric rating? (Choose two.)

- [ ] A. The Security Fabric rating is a free service that comes bundled with all FortiGate devices.
- [ ] B. Many of the security issues can be fixed immediately by clicking Apply where available.
- [ ] C. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric.
- [ ] D. It provides executive summaries of the four largest areas of security focus.

Answer(s): B C

---

11. An administrator has configured outgoing interface any in a firewall policy.
Which statement is true about the policy list view?

A. Interface Pair view will be disabled.

B. Search option will be disabled.

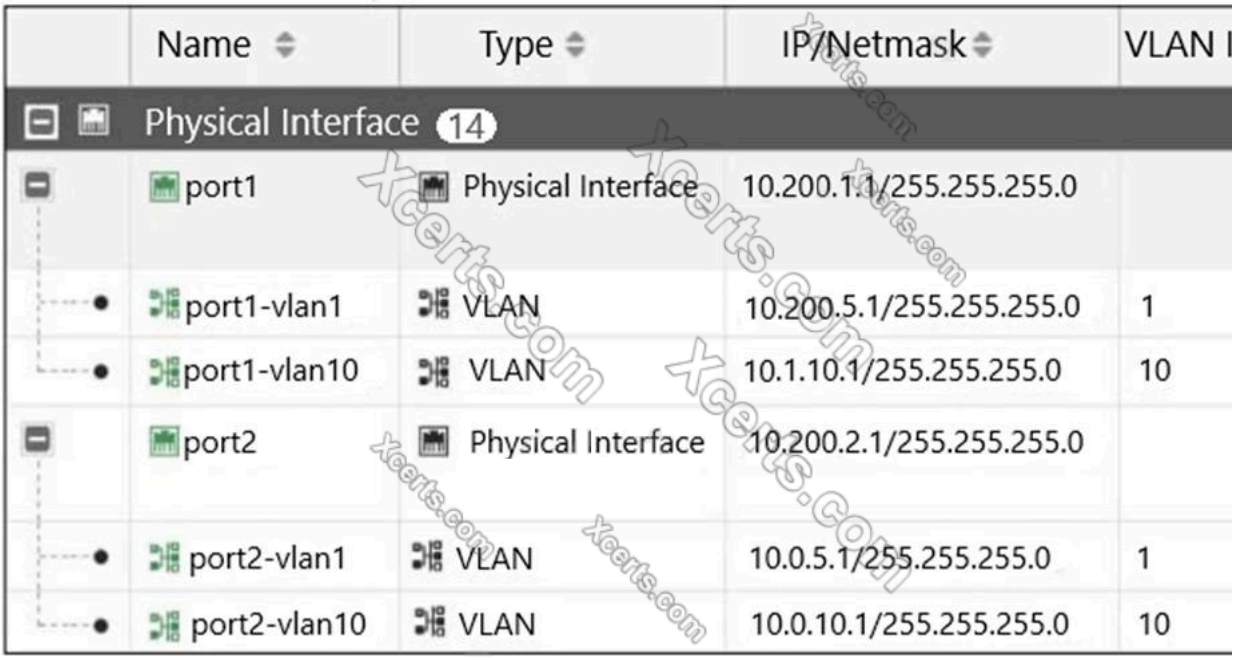
C. Policy lookup will be disabled.

D. By Sequence view will be disabled.

Answer(s): A

---

12. Refer to the exhibit.



	Name	Type	IP/Netmask	VLAN I
Physical Interface 14				
	port1	Physical Interface	10.200.1.1/255.255.255.0	
	port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
	port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
	port2	Physical Interface	10.200.2.1/255.255.255.0	
	port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1
	port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10

Given the interfaces shown in the exhibit, which two statements are true? (Choose two.)

- ☐ A. Traffic between port2 and port2-vlan1 is allowed by default.
- ☐ B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
- ☐ C. port1-vlan1 and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.
- ☐ D. port1 is a native VLAN.

Answer(s): C D

---

13. A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.
-All traffic must be routed through the primary tunnel when both tunnels are up
-The secondary tunnel must be used only if the primary tunnel goes down
-In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover
Which two key configuration changes are needed in FortiGate to meet the design requirements? (Choose two.)

- ☐ A. Configure a higher distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.
- ☐ B. Enable Dead Peer Detection.
- ☐ C. Enable Auto-negotiate and Auto Keep Alive on the phase 2 configuration of both tunnels.
- ☐ D. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.

Answer(s): B D

---

14. Refer to the exhibit.

```
vcluster_nr=1
vcluster_0: start_time=1593701974(2021-06-02 10:59:34), state/o/chg_time=2(work)/2(work)/
        pingsvr_flip_timeout/expire=3600s/2781s        2021-06-02
        'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=0x0000
        'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=0x0000
```

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster.
The override setting is enable for the FortiGate with SN FGVM010000064692.
Which two statements are true? (Choose two.)

- [ ] A. FortiGate SN FGVM010000065036 HA uptime has been reset.
- [ ] B. FortiGate devices are not in sync because one device is down.
- [ ] C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.
- [ ] D. FortiGate SN FGVM010000064692 has the higher HA priority.

Answer(s): A D

---

15. Refer to the exhibits.
Exhibit A shows system performance output.

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softi
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% soft
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 ses
Average session setup rate: 0 sessions per second in last 1 minute, 0 ses
10 minutes, 0 sessions per second in last 30 minutes,
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days,  3 hours,  28 minutes
```

Exhibit B shows s FortiGate configured with the default configuration of high memory usage thresholds.

```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

Based on the system performance output, which two statements are correct? (Choose two.)

- [ ] A. FortiGate will start sending all files to FortiSandbox for inspection.
- [ ] B. FortiGate has entered conserve mode.
- [ ] C. Administrators cannot change the configuration.
- [ ] D. Administrators can access FortiGate only through the console port.

Answer(s): B C

---

16. An administrator is configuring an IPsec VPN between site A and site B. The Remote Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is

192.168.1.0/24 and the remote quick mode selector is 192.168.2.0/24.
Which subnet must the administrator configure for the local quick mode selector for site B?

A. 192.168.3.0/24

B. 192.168.1.0/24

C. 192.168.0.0/8

D. 192.168.2.0/24

Answer(s): D

---

17. Refer to the exhibits.
Exhibit A.

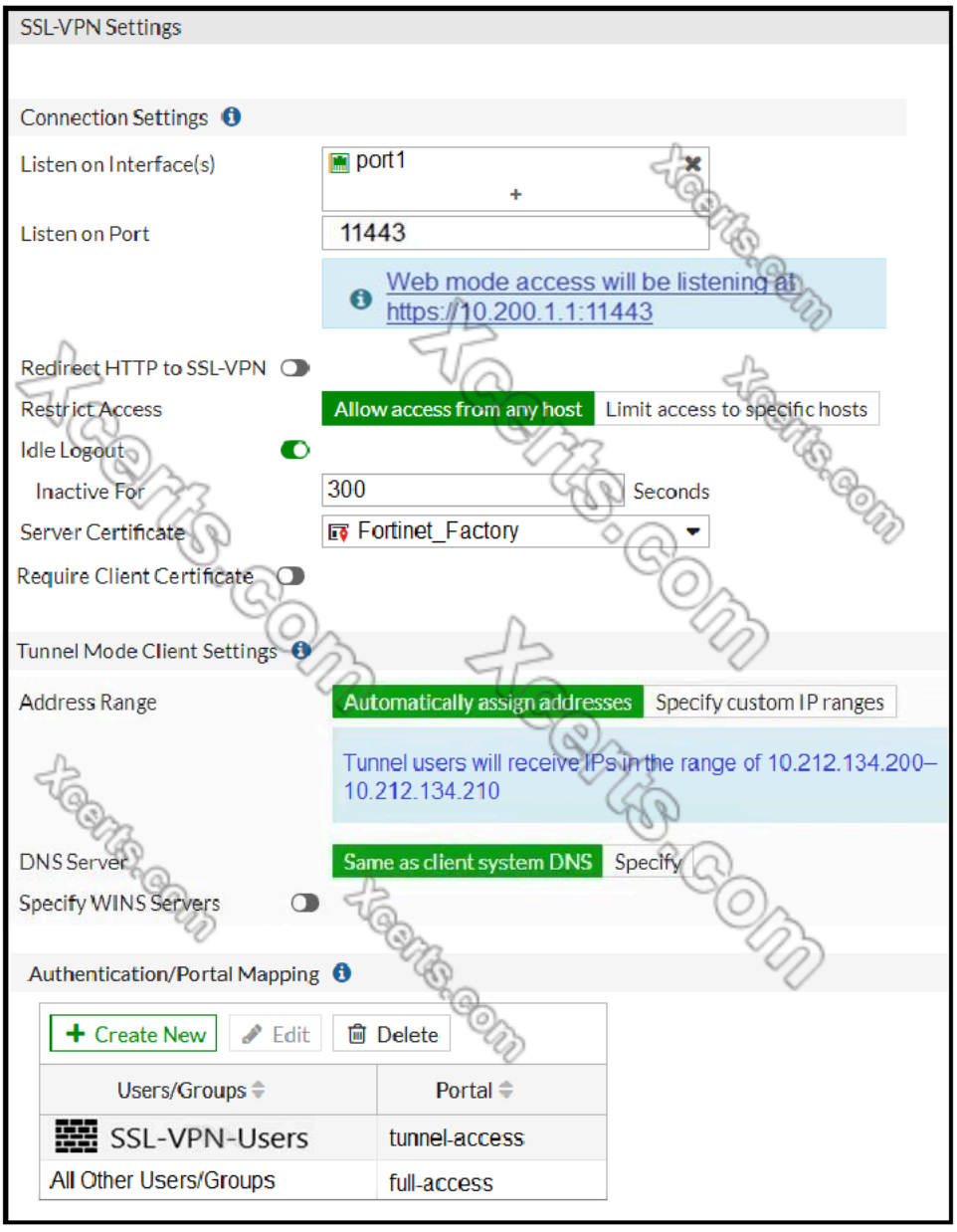


Exhibit B.

The SSL VPN connection fails when a user attempts to connect to it.
What should the user do to successfully connect to SSL VPN?

A. Change the SSL VPN port on the client.

B. Change the Server IP address.

C. Change the idle-timeout.

D. Change the Server IP address.

Answer(s): A

---

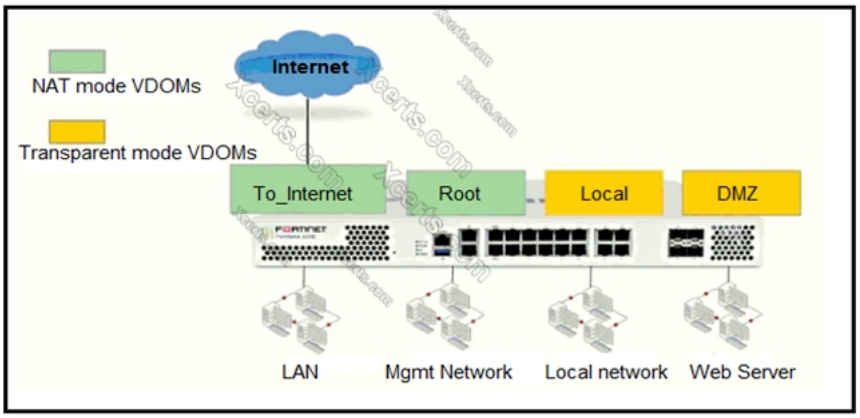
18. Which two statements about SSL VPN between two FortiGate devices are true? (Choose two.)

- [ ] A. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
- [ ] B. The client FortiGate requires a manually added route to remote subnets.
- [ ] C. The client FortiGate uses the SSL VPN tunnel interface type to connect SSL VPN.
- [ ] D. Server FortiGate requires a CA certificate to verify the client FortiGate certificate.

Answer(s): C D

---

19. Refer to the exhibit.



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.
The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem.
With this configuration, which statement is true?

A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.

B. A default static route is not required on the To_Internet VDOM to allow LAN users to access the internet.

C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.

D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Answer(s): A

---

20. Refer to the exhibits.
Exhibit A.

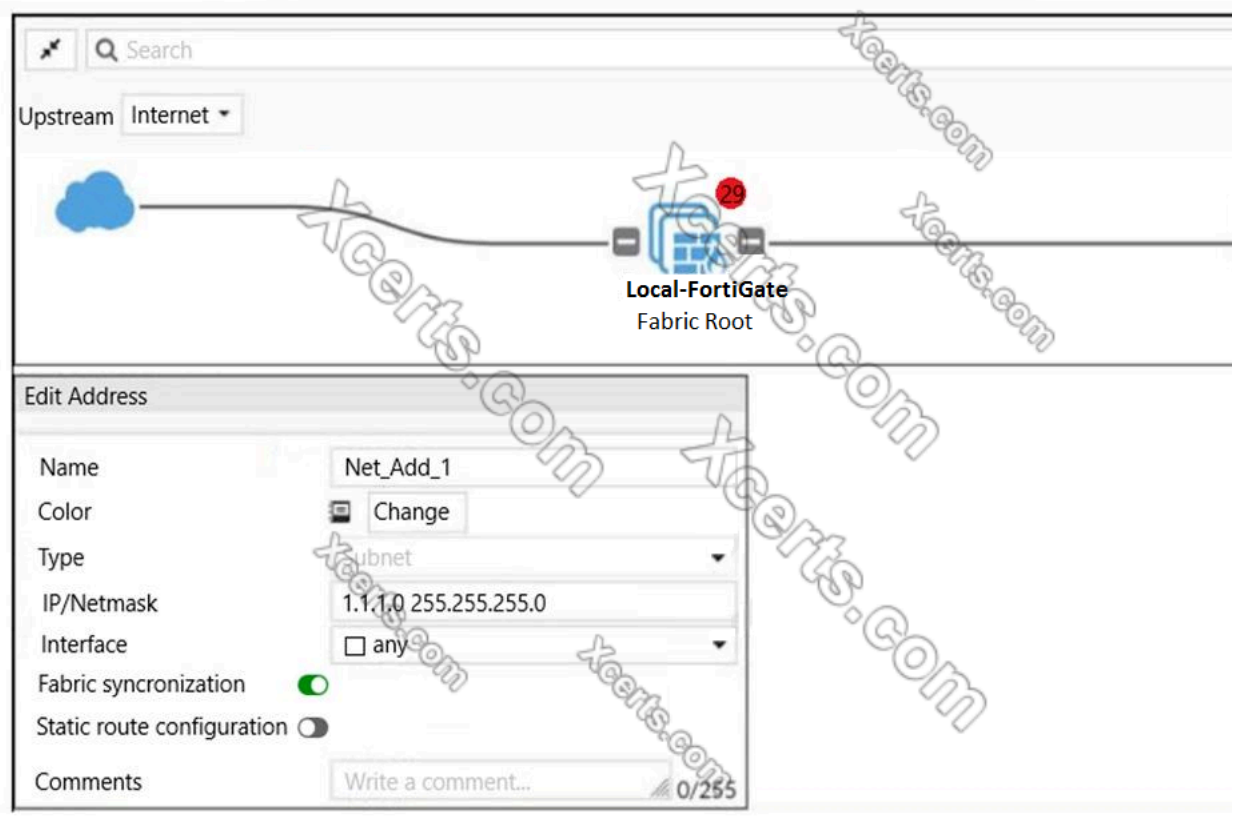


Exhibit B.

```
Local-FortiGate # show full-configuration system csf
config system csf
    set status enable
    set upstream-ip 0.0.0.0
    set upstream-port 8013
    set group-name "fortinet"
    set group-password ENC X18CtzrcUBUq9yz9nryP+YfM16
BJkv7S/trtoh2gYAe5CH8YMAa0GT18aX+/dKH/o5izw1ZEoN1QN2N
FGLT4r5z2AyYI8i1PxutiLcsCp1AdZadv1CxDe66IdLX7I6o22J9P
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set fabric-object-unification local
    set saml=configuration-sync default
```

```
ISFW # show full-configuration system csf
config system csf
    set status enable
    set upstream-ip 10.0.1.254
    set upstream-port 8013
    set group-name ''
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set saml-configuration-sync default
end

ISFW #
ISFW #
```

An administrator creates a new address object on the root FortiGate (Local-FortiGate) in the security fabric. After synchronization, this object is not available on the downstream FortiGate (ISFW).
What must the administrator do to synchronize the address object?

A. Change the csf setting on Local-FortiGate (root) to set configuration-sync local.

B. Change the csf setting on ISFW (downstream) to set configuration-sync local.

C. Change the csf setting on Local-FortiGate (root) to set fabric-object-unification default.

D. Change the csf setting on ISFW (downstream) to set fabric-object-unification default.

Answer(s): A
